IN THE U.S. PATENT AND TRADEMARK OFFICE

Application No.:	10/549,407
Filing Date:	September 14, 2005
Applicant:	Junbiao ZHANG et al.
Group Art Unit:	2431
Confirmation No.:	1695
Examiner:	Shin Hon CHEN
Title:	AUTOMATIC CONFIGURATION OF CLIENT TERMINAL IN PUBLIC HOT SPOT
Attorney Docket:	PU030084

APPELLANTS' BRIEF ON APPEAL

MAIL STOP APPEAL BRIEF - PATENTS
Customer Service Window
Randolph Building
401 Dulany Street
Alexandria, VA 22314

September 28, 2009

TABLE OF CONTENTS

APPELLANTS' BRIEF ON APPEAL

I. REAL PARTY IN INTEREST:

The real party in interest in this appeal is Thomson Licensing S. A. Assignment of the application was submitted to the U.S. Patent and Trademark Office and recorded at Reel 016990, Frame 0204.

II. RELATED APPEALS AND INTERFERENCES:

There are no known appeals or interferences that will affect, be directly affected by, or have a bearing on the Board's decision in this Appeal.

III. STATUS OF CLAIMS:

Claims 1-31 are pending in the application, with claims 1, 5, 7, 21 and 24 being written in independent form.

Claims 1-31 remain finally rejected under 35 U.S.C. §102 as being anticipated by Luo, U.S. Pub. No. 2003/0169713 (hereinafter Luo). Claims 1-31 are being appealed.

IV. STATUS OF AMENDMENTS:

A Request for Reconsideration ("Request") was filed on June 23, 2009. In an Advisory Action dated July 6, 2009, the Examiner stated that the Request was considered but did not place the application in condition for allowance. An amendment submitted with the Request to place the claims in better form for appeal under Rule 116 was not entered. After the filing of a Notice of Appeal on July 7, 2009 and refiling the Request, the Examiner issued a second Advisory Action on July 15, 2009, entering the amendment submitted with the Request.

V. SUMMARY OF CLAIMED SUBJECT MATTER:

(i). Overview of the Subject Matter of the Independent Claims

The present invention is directed at methods, an access point and a mobile terminal depicted in Figures 1-3. A communications block diagram is provided by FIG. 1, a flow diagram of the methods in FIG. 2 and details of the access point 130_n and terminal 140_n are shown in FIG. 3. Access point independent claim 5, mobile terminal independent claim 21 and access point independent claim 24 are written with "means plus function elements" whose supporting and equivalent structure is described in the Specification/Drawings. Reference should also be made to FIG. 2 for independent method claims 1 and 7. More specifically, independent claim 1 reads as follows (Specification/Drawing reference character citations are in parenthesis):

1. A method for enabling a client terminal (140_n) to access a wireless network (115, 124), comprising:
receiving an access request (220, 325, 230; 355) from the client terminal;
redirecting (325, 335, 345; 418, 420, 422) the access request to a local web server (120) via a packet traffic filter (330, 420) for filtering packet traffic;
requesting (355, 360) from the client terminal, information to establish client terminal access to the wireless network;
activating (370), in response to the client terminal access information received from the client terminal, a module (465) that reconfigures (375) the client terminal for authentication using appropriate parameters associated with a configuration arrangement (450, 448) selected by a user; and
authenticating (425) the reconfigured client terminal and allowing access (427) to the wireless network in response to the authentication.

Each element identified in independent claim 1 and each subsequent independent claim will now be specifically identified as to page and line number of the specification, as appropriate, and to drawing by drawing number. Page

and line number will be provided from a preliminary amendment (PA) to the specification filed September 15, 2005, if the referenced paragraph replaces the original paragraph.

In particular with respect to independent claim 1, client terminal 140_n is described throughout the specification beginning at page 1, lines 9-14; page 2, line 25 through page 8, line 24 where the client terminal is referred to, for example, as "IEEE 802.1 client" at page 4, lines 20-30, "terminal" at page 4, lines 31 to page 5, line 7, and "mobile terminals" at page 5, lines 8-14 and depicted in each drawing of Figures 1-3. Wireless network 115, 124 is likewise described throughout the specification beginning at page 1, lines 9-14; page 2, line 25 through page 8, line 24 where the wireless network is referred to as "communications network," "WLAN" (wireless local area network), "WLAN architecture" or "WLAN environment" (page 5, lines 15-28) and depicted in Figures 1 and 3.

Redirecting is performed by 802.1X Engine 325 as described at page 6, line 12 (PA) through page 6, line 29 and depicted in FIG. 2. Redirecting function 335, 345 is described at page 6, line 29 (PA) through page 7, line 7 and depicted in FIG. 2. Redirecting processors 418, 420, 422 are described at page 7, line 30 (PA) through page 8, line 15 and are depicted in FIG. 3.

Local web server 120 is described throughout the specification, for example, as "web server" beginning at page 2, line 25, through page 3, line 31 and as "local web server," "HTTP server" or "web server" beginning at page 4, line 20 to page 5, line 9 and "local web server" at page 8, line 15; "HTTP server 120_n" at page 6, line 2, "HTTP server 120" at page 6, line 17, at page 7, line 9 (PA) and page 7, line 11 and "designated web server 120" at page 7, line 18 (PA) and "web server 120" at page 7, line 29, and is depicted in FIG. 1 and 2.

Packet traffic filter 330, 420 is introduced beginning at page 6, line 17 as "packet filtering function 330" and "packet filter module 330" at page 6, line 30 and page 7, line 7 (PA) and is depicted in FIG. 2 and also is described as "packet

filter module 420" or "packet filter 420" beginning at page 7, line 34 and depicted in FIG. 3.

Requesting 355, 360 is introduced as "requests access" at page 3, line 21 and at page 7, line 17 (PA) and a provider list web page 360 is the response at page 7, line 20 (PA) and depicted in FIG. 2.

Activating 370 is introduced at page 2, line 29; page 3, line 26 (PA); page 4, line 33 to page 5, line 7 and page 7, line 33 (PA) and the paragraph beginning at page 7, line 30 (PA) with respect to "ActiveX" and is depicted in FIG. 2. A "module" 465 or reconf(igure) means 465 is shown in FIG. 3 while reconfigures (the function) 375 is described, for example, as "reconfiguring 375" at page 7, line 33 and is depicted in FIG. 2.

Configuration arrangement 450, 448 is described in the paragraph beginning at page 7, line 30 (PA) and depicted in FIG. 3.

Authenticating 425 is described in the paragraph beginning at page 7, line 30 (PA) and depicted in FIG. 3.

Allowing access 427 is also described in the paragraph beginning at page 7, line 30 (PA) and depicted in FIG. 3.

Independent claim 5 reads as follows:

5. An access point (130_n) for providing a secure communications session between a client terminal (140_n) and a wireless network (115, 124), comprising:

means (330, 355; 415, 418) for receiving an access request from the client terminal;

means (330, 345; 418, 420, 422) for redirecting the access request to a local web server (120) for allowing a reconfigured access to the wireless network via a packet filter means (330, 420) for filtering packet traffic,

means (325, 350, 335 (EAP Failure)) for requesting from the client terminal, information to establish client terminal access to the wireless network;

means (330, 345; 420) for activating, in response to the client terminal access information (355) received from the client terminal, a software module (465) that reconfigures the client terminal for

authentication using appropriate parameters associated with a configuration arrangement (450, 448) selected by a user; and

means (425) for authenticating the reconfigured client terminal and allowing access (427) to the wireless network in response to the authentication.

Only newly claimed elements will be discussed as to specification and drawing citations for claim 5. While the claim is in means plus function format, the referenced means by reference numeral have already been discussed above in many instances. Access point 130_n is described throughout the specification and is first described as "WLAN AP" where AP is access point at page 5, line 4, as "access point AP" at page 5, line 9 and "AP stations" at page 5, line 17 and are depicted in Figures 1-3.

Means for receiving an access request is exemplified by packet filter module 330, 420 shown respectively in FIG. 2 and 3. The function of receiving is depicted as web access request 355 in FIG. 2. Receiver 415 receives the access request at the access point 130_n and it is processed at access request processor 418 of FIG. 3.

Means for redirecting is packet filter module 330, 420 as discussed above and depicted in FIG. 2-3.

Means for requesting relates to an EAP or state failure mode, and the 802.1X engine 325 in particular is the representative means as seen in FIG. 2 and described at the paragraph beginning at page 6, line 29 (PA).

Means for activating is the packet filter module 330, 420.

Means for authenticating is the means 425 shown in FIG. 3.

Independent claim 7 reads as follows:

7. A method for configuring a client terminal (140_n) to provide secure access in a wireless network (115), comprising:

filtering (330; 420) traffic associated with a request (210, 220; 335) from the client terminal for access to the wireless network, at a packet traffic filter (330, 420) for filtering packet traffic;

redirecting (345) the access request to a designated web server (120), via said packet traffic filter for filtering packet traffic; and

issuing (120; 360) a provider list web page and a request from the designated web server to the client terminal for provider selection information (365) to establish an authorized communication.

Filtering and redirecting have already been discussed above. Issuing a provider list web page is shown as 360 in FIG. 2 and is performed by HTTP server 120 per the paragraph beginning at page 7, line 13 (PA).

Independent claim 21 reads as follows:

21. A mobile terminal (140_n), comprising:
means (445) for receiving an extended authentication protocol request identification message packet (210);
means (470) for forwarding an extended authentication protocol response identity message packet (220);
means (445) for receiving an extended authentication protocol failure message packet (335 (EAP Failure));
means (470) for forwarding a web access request (355) via a packet traffic filter (330; 420) for filtering packet traffic as a web request redirect message (345; 422);
means (445) for receiving a provider list web page (360);
means (450; 448) for selecting a provider and means (470) for forwarding selected provider information (365) to a designated web server (120);
means (445; 370) for receiving an ActiveX control/plug-in from the designated web server to reconfigure (375) said mobile terminal; and
means (465) for reconfiguring said mobile terminal and establishing authorized communications.

Claim 21 relates to means plus function elements which are primarily client receiver and transmitter elements of FIG. 3 acting in functional sequence according to FIG. 2. Means 445 for receiving an EAP packet 210 at a mobile terminal is receiver 445 shown in FIG. 3 where the packet 210 is shown in FIG. 2. Means 470 is depicted as transmitter 470 of FIG. 3 with the packet 220 shown in FIG. 2. Similarly, EAP failure has no reference number but is near function 335 in FIG. 2. Web request redirect is function 345 of FIG. 2. Means for selecting is a client input means 450 depicted in FIG. 3. The selected provider information is depicted as function 365 in FIG. 2. Means for

reconfiguring 465 is the Reconf means 465 depicted in FIG. 3 and the reconfiguration is function 375 shown in FIG. 2.

Independent claim 24 reads as follows:

24. An access point (130_n) associated with a communications network (115), comprising:

means (325; 424) for forwarding an extended authentication protocol request identification message packet (210) to a client terminal (140_n);

means (325; 415) for receiving an extended authentication protocol response identity message packet (220) from the client terminal;

means (325; 424) for forwarding an extended authentication protocol failure message packet (335 EAP Failure) to the client terminal responsive to a state failure (350);

means (330; 415, 422) for receiving a re-direct client request (335) from said forwarding means at a packet filter module (330; 420) responsive to said state failure;

alternative means (330; 420; 415, 418) for receiving a request for access (355) to a communications network (115) at said packet filter module responsive to said state failure; and

means (330; 420, 422, 424) for forwarding a web request redirect (345) from said packet filter module (330; 420) to a designated web server (120) for establishing authorized communications following receipt (365) of selected provider information at the designated web server and successful client terminal reconfiguration (375) responsive to authentication.

Means 325 (802.1X Engine) and 330, 420 (packet filter module) have been discussed above. The alternative means is described in the paragraph beginning at page 6, line 29 (PA) and is represented by packet filter module 330 of FIG. 2 and 420 of FIG. 3. All other means have already been discussed above.

In order to make the overview set forth above concise, the disclosure that has been included, or referred to, above only represents a portion of the total disclosure set forth in the Specification/Drawings that supports the independent claims. Moreover, the Board is asked to consider features of dependent claims 2-4, 6-12, 14-15, 19 and 28-31 as well as to consider

dependent claims 13, 16-18, 20, 22-23 and 25-27 as standing on the merits of claims on which they depend.

In particular, by way of example, dependent claims 2, 6 and 8 relate to an IEEE 802.1 or an 802.11 compliant terminal/network, while Luo admits that the standard at the time of Luo's invention was under development [0007]. Dependent claims 3, 4, 19, 30 relate in part to an ActiveX control which the Examiner equates to a Java applet. As will be further explained below, the Luo Java applet functionally differs from the recited ActiveX control and so does not comprise an equivalent structure.

By way of further example, dependent claims 9 and 28-29 relate to provider selection information not discussed in Luo.

(ii). The Remainder of the Specification Also Supports the Claims

The Appellants note that there may be additional disclosure in the Specification/Drawings that also supports the independent and dependent claims. Further, by including the specification/drawing citations in parenthesis above the Appellants do not represent that this is the only evidence that supports the independent (or dependent) claims nor do Appellants necessarily represent that these citations alone can be used to fully interpret the claims. Instead, the citations provide background support as an overview of the claimed subject matter.

VI. GROUNDS OF REJECTION TO BE REVIEWED ON APPEAL:

Appellants seek the Board's review and reversal of the rejection of claims 1-31 based on 35 U.S.C. §102.

VII. ARGUMENTS:

A. The Section 102 Rejection Based on Anticipation

In the Final Office Action issued April 28, 2009, claims 1-31 stand rejected under 35 U.S.C. § 102 as allegedly anticipated by Luo. The Examiner states at Page 11: "Although Luo does not provide word-for-word disclosure of certain claimed limitation Luo discloses inherent and underlying functionality as claimed by applicant. Furthermore, applicant mainly argues that the prior art of record discloses non-standard protocol rather than standard protocol and argues that the difference can be demonstrated by referring to the Specification. However, the examiner rejected the claims based on broadest reasonable interpretation and the claims are not deemed to overcome the prior art of record" (our emphasis added).

On the Continuation Sheet (PTO-303) attached to his Advisory Actions of July 6 and 15, 2009, the Examiner again sets forth his reliance on the standard of "broadest reasonable interpretation" for rejecting the claims. The Examiner also states his reliance on "802.1x protocol" as "well known and developed at the time of applicant's invention." However, the burden of proof is on the Examiner to demonstrate anticipation. The Examiner has not provided a copy of "802.1x protocol" and his allegation that the protocol was "well known and developed at the time of applicant's invention" is pure argument and not based in fact.

The Examiner has applied incorrect principles of law in his anticipation rejection. The proper test for "anticipation" is set forth in *NetMoneyin, Inc. v. Verisign, Inc. et al.*, decided less than eight months ago, October 20, 2008, (545 F. 3rd 1359, at 1369):

> Section 102(a) provides that an issued patent is invalid if "the invention [therein] was . . . described in a printed publication . . . before the invention thereof by the applicant." Section 102 embodies the concept of novelty—if a device or process has been previously invented (and disclosed to the public), then it is not

> new, and therefore the claimed invention is "anticipated" by the prior invention. As we have stated numerous times (language on which Verisign relies), in order to demonstrate anticipation, the proponent must show "that the four corners of a single prior art document describe every element of the claimed invention" (citations omitted). This statement embodies the requirement in section 102 that the anticipating invention be "described in a printed publication," and is, of course, unimpeachable. But it does not tell the whole story. Because the hallmark of anticipation is prior invention, the prior art reference – in order to anticipate under 35 U.S.C. 102 – **must not only disclose all elements of the claim within the four corners of the document, but also disclose those elements "arranged as in the claim,"** (citation omitted) (our emphasis added).

Moreover, "[w]hile claim terms are given their broadest reasonable interpretation during examination, that interpretation must be consistent with the specification," (our emphasis added) *In re Prater,* 415 F.2d 1393, 1404 (CCPA). "It is well settled that a prior art reference may anticipate when the claim limitations not expressly found in that reference are nonetheless inherent in it. Under the principles of inherency, if the prior art necessarily functions in accordance with, or includes, the claim limitations, it anticipates." *In re Cruciferous Sprout Litig.,* 301 F.3d 1343, 1349 (Fed. Cir. 2002). "Inherency, however, may not be established by probabilities or possibilities. The mere fact that a certain thing may result from a given set of circumstances is not sufficient" (our emphasis added). *In re Robertson,* 169 F.3rd 743, 745 (Fed. Cir. 1999).

By way of brief summary and by way of example, the Examiner equates a "packet traffic filter" feature with a functional description in Luo at [0022] and [0023] where Luo's passing of certain packets while others are blocked in a "limited" routing state is necessarily equated with an "access request" and a "packet traffic filter" as recited. This is but one example of "probabilities" or "possibilities" that Luo anticipates the independent claims but not necessarily

actualities. Other examples will be discussed below in order as presented in the final office action.

Claims 1 and 5

With respect to independent claims 1 and 5, Applicants, for example, direct attention to "redirecting the access request to a local web server via a packet traffic filter for filtering packet traffic." Claim 1 is a method claim and claim 5 is in means plus function format.

Firstly, a means "for redirecting" is recited within the claim element as a "packet traffic filter for filtering packet traffic." Luo fails to specifically discuss or suggest a packet traffic filter, only a related function as further described below.

The Examiner points to Luo [0018] which is completely silent about "redirecting" "to a local web server" and "via a packet traffic filter for filtering packet traffic." Moreover, claim 1 reads "receiving an access request from the client terminal" followed by "redirecting." Consequently, the "redirecting" is not occurring at the client terminal (Luo's mobile host). It is occurring where a recited "packet traffic filter" is located. Luo shows a mobile access point 102 which is probably the "access point" referred to in [0023].

In his **Response to Arguments** Page 10, 33., the Examiner points to Luo [0023] and states as follows: "Luo discloses that certain packets are allowed to pass through while others are filtered based on state information." This interpretation fails to establish a *prima facie* case of anticipation on several counts. Firstly, Luo [0023] fails to disclose or suggest what happens to an "access request," secondly, that the access request is redirected, thirdly, that when the access request is redirected, the access request is redirected to a "local web server" and, fourthly, that the redirecting of the access request is "via a packet traffic filter for filtering packet traffic."

Luo [0021] states: "MAP's 102 (mobile access points) are responsible for access control;" however, thereafter, Luo [0023] clearly indicates that whatever

function is performed regarding passing and blocking "frames" is performed as a condition of the mobile host's routing state. There is no discussion of what happens to an "access request." Luo uses the term "MH associates with MAP" – mobile host associates with mobile access point at 200 of Fig. 2. Luo states:

> "The mobile host's routing state is set to 'normal,' 'limited' or 'blocked.' The 'normal' state means that the mobile host has been authenticated . . . the access point will relay all frames that are communicated to or from the mobile host. A 'limited' state means . . . the access point should block all frames except those carrying IP configuration packets . . . between the mobile host and the WLAN, DNS (domain name server) packets between the mobile host and the conditional DNS server, and HTTP packets between the mobile host and the web-based authentication server." "A 'blocked' state means . . . the access point will block all frames sent to and from the mobile host."

A possible interpretation of Luo is that in a "limited" state some frames carrying IP configuration packets, domain name server packets and HTTP packets are passed. But, if the Examiner for the purposes of discussion interprets this "limited" state involves a packet traffic filter as broadly interpreted but inconsistently with the present specification, these types of packets are not an "access request" that is "redirected" to a local web server.

Per the present specification, a rejected Radius Access Request results in a failure 350 and a redirect 335, 345 to HTTP server 120 via packet filter module 330.

To the contrary and according to Luo, DNS and HTTP packets are passed, according to Luo, to one of a conditional DNS server and a Web-based authentication server. Consequently, Luo functionally differs from the present specification and the features of claims 1 and 5. Claims 1 and 5 must be interpreted consistently with the Specification/Drawings and Luo fails to anticipate claims 1 and 5.

In summary then, it is not clear from Luo "within the four corners of the document" that "redirecting the access request to a local web server via a packet traffic filter for filtering packet traffic" is performed.

The next elements when read together read as follows: "requesting from the client terminal, information to establish client terminal access to the wireless network; activating, in response to the client terminal access information received from the client terminal, a module that reconfigures the client terminal for authentication using appropriate parameters associated with a configuration arrangement selected by the user; and authenticating the reconfigured client terminal and allowing access to the client network in response to the authentication."

Luo operates differently. The Examiner points vaguely to Luo [0043] for "requesting . . .," "submitting credentials"; Luo [0018] for "activating . . ." "other accounts the user has" and Luo [0045] for the "Java applet/appropriate parameters." The Examiner also relies on Luo [0045] for "authenticating the reconfigured terminal . . ." "grant access after applet is activated" while claims 1 and 5 specifically read as above, must be read consistently in view of the Specification/Drawings and so differ from Luo.

For example, Luo Fig. 2 208 states "MH runs DHCP to receive IP address and network configuration parameters from MAP." In particular, at [0038], "The mobile host then runs DHCP to obtain an IP address and other network configuration parameters from the MAP at 208" (Luo Fig. 2). It is not until step 238 of Fig. 2 that "Web auth. Server sends Java applet to MH." Consequently, since it appears that the Examiner is equating the Luo Java applet to the function of a "module that reconfigures," the Examiner is precluded from assuming that Luo performs "activating, in response to the client terminal access information received from the client terminal, a module that reconfigures the client terminal for authentication using appropriate parameters associated with a configuration arrangement selected by the user"

where the sending of a Java applet at 238 is the last block of the Luo process Fig. 2 and parameters come earlier from the MAP at 208 (not from the user). Luo has no module that reconfigures the client terminal using appropriate parameters associated with a configuration arrangement selected by the user.

Rather, the Luo user launches his web browser [0037] and enters, for example, www.att.com, enters the limited state [0038], and the user can submit authentication credentials [0043], all without the Java applet, introduced at [0045].

Luo paragraphs [0045] and [0046] are telling:

> At 236 the small browser window will automatically send the fourth HTTP request message over SSL to the Web authentication server to download a Java applet. After the Java applet is downloaded at 238, it grants some networking privileges so that it can listen to a specific UDP port for AUTHENTICATION CHALLENGE messages. The Java applet shares a high entropy secret with the Web authentication server, which can then be used to generate AUTHENTICATION RESPONSE messages.
> The mobile host can now use the assigned IP address during the entire session as long as it is under the coverage of the WLAN. The user should keep this small browser window always open. The Java applet runs in this small browser window and authenticates the user to the WLAN as the user moves from one MAP to another, (our emphasis added).

Luo has no reconfiguration module as recited, let alone, using appropriate parameters associated with a configuration arrangement selected by a user. Luo's Java applet is not activated in response to the client terminal access information received from the client terminal as recited. It is downloaded at the end of the process via access point provided parameters and operates in a window that must be forever open.

Reversal of the anticipation rejection of claims 1 and 5 is respectfully requested.

Claims 2, 6 and 8

At Page 3, the Examiner rejects claims 2 and 6 whereby, for example, the feature of an IEEE 802.11 compliant wireless local area network is recited. Luo admits at [0007], "To address the security flaws associated with WEP, the IEEE 802.1x standard has been introduced and **the IEEE 802.11i standard is currently under development.**" (our emphasis added). It is respectfully submitted that Luo cannot comply with a moving target where the claim refers to 802.11 circa Zhang's filing date of 2005. Luo without further support from the Examiner must be read in view of its filing date as to the status of 802.11. Claim 8, dependent on independent claim 7, is not anticipated by Luo for the same reasons as claims 2 and 6 in addition to the reasons why claim 7 is not anticipated as discussed below. Reversal of the anticipation rejection of dependent claim 2/1, 6/5 and 8/7 is respectfully requested.

Claims 3, 19, 20, 30 and 31

At Page 3, the Examiner refers to Luo [0018] and [0045] for "activating an ActiveX control plug-in installed on the client terminal." Luo describes "a Java applet" or "an equivalent client-side program delivered by the Web page" at [0018]. The Examiner appears to be equating ActiveX perfectly with "a Java applet (or an equivalent client-side program delivered by the web page and installed by the user)" [0018] but the ActiveX as recited functions differently. Luo's equivalent does not, for example, reconfigure "the client terminal for authentication using appropriate parameters associated with a configuration arrangement selected by a user" as described above. The Luo Java applet is downloaded at step 236 and parameters for limited access are provided from the access point. Pointing one's browser at AT&T is not the same as "appropriate parameters associated with a configuration arrangement selected by a user." When claim 3 is read in conjunction with claim 1, claim 19 read in conjunction with claims 9 and 7 (discussed subsequently herein), claim 20 read in conjunction with claims 8 and 7, claim 30 read in conjunction with

claim 21 and claim 31 read in conjunction with claim 24, the Luo Java applet is not, for example, a "module that reconfigures the client terminal for authentication using appropriate parameters associated with a configuration arrangement selected by a user." Consequently, reversal of the anticipation rejection of claims 3, 19, 20, 30 and 31 is respectfully requested.

Claim 4

Again, the Examiner appears to equate the Java applet downloaded at step 236 with a recited ActiveX plug-in. For similar reasons that claim 3 is not functionally anticipated, neither is claim 4. Consequently, reversal of the anticipation rejection of claim 4 is respectfully requested.

Claim 7

Independent method claim 7 comprises "filtering" and "redirecting" which are discussed above with respect to claims 1 and 5. These features are not taught by Luo and so Luo can not anticipate claim 7 for at least the reasons stated above. Claim 7 further recites "issuing a provider list web page and a request from the designated web server to the client terminal for provider selection information to establish an authorized communication," which feature is not described by Luo. To the contrary, Luo [0037] states that the user launches his web browser . . . specifies a non-blank page . . . such as 'http://www.att.com'" and so on. Luo [0018] states "new users can open accounts . . . or refer the Web-based authentication server to other authentication servers where they have accounts." However, Luo fails to disclose or suggest "issuing a provider list web page and a request from the designated web server to the client terminal for provider selection information to establish an authorized communication" as recited. Consequently, for this further reason as well as the reasons stated above, reversal of the anticipation rejection of claim 7 is respectfully requested.

Claim 9

Claim 9 depends from claim 7 and recites "the designated web server receiving from the client terminal said provider selection information for establishing said authorized communication" where the "designated web server" is not a Luo "authentication server;" see Luo 202, 214, 216, 220. The Luo authentication server is not a designated web server which issues a provider list web page and a request per claim 7. Reversal of the anticipation rejection of claim 9 is respectfully requested.

Claims 10-18

Claims 10-18 which depend directly or indirectly on claim 9 correspond to the wording used in a (amended) replacement paragraph beginning at page 7, line 13, as follows: "In the course of the communication the web server 120 indicates to client terminal 140_n information corresponding to such parameters as transmission rates (claim 10/9/7), user account creation information (claim 11/9/7), authentication method selection information (claim 12/9/7 and claim 17/12/9/7), new account creation procedures (claim 13/9/7 and claim 16/11/9/7), access user terms as conditions of acceptance (claim 14/9/7 and claim 18/14/9/7), access rate information (claim 15/10/9/7) all typically required to establish an authorized communication. The client terminal 140_n user responds (365 in FIG. 2), accordingly communicating web server 120, access rate information (claim 15), web server user account creation information (claim 16), user access authentication method selection information (claim 17), and user access terms and conditions of acceptance information (claim 18) required to establish an authorized communication," (Applicants' indication of claim numbers added). The Examiner submits that recited establishment of an authorized communication of dependent claims 10-18 may be suggested by Luo's statement: "new users can open accounts" at Luo paragraph [0018]. However, this statement is clearly not an enabling disclosure of dependent claims 10-18. The Examiner is relying at best on a

"possibility," not "inherency" and so Applicants respectfully request that the anticipation rejection of claims 10-18 be reversed.

Claim 21

Claim 21 is an independent claim directed to a "mobile terminal" (not described by Luo) at least as comprising: "means for forwarding a web access request via a packet traffic filter for filtering packet traffic as a web request redirect message; means for receiving a provider list web page; means for selecting a provider and means for forwarding selected provider information to a designated web server; means for receiving an ActiveX control/plug-in from the designated web server to reconfigure said mobile terminal; and means for reconfiguring said mobile terminal and establishing authorized communications." Luo does not describe any of these means. For example, Luo [0040] describes "a short HTTP response message that contains a redirect URL pointing to the SSL (Secure Socket Layer) port of itself." This is not the respective means "arranged as in the claim" as recited and when construed in compliance with 35 U.S.C. 112, sixth paragraph. Consequently, applicants respectfully request that the anticipation rejection of claim 21 be withdrawn.

Claims 22-23 and 25-27

Claim 22 dependent on claim 1 reads: "creating a plurality of operational states including a progress state and a failure state, said packet traffic filter receiving wireless local area network failure state information via a redirect client message and moves a reconfiguration process to said local web server via a web request redirect message." Claim 25 dependent on claim 1, for example reads: "detecting a state failure responsive to receipt of an EAP response identity packet and to receipt of a RADIUS access reject message." Claim 23 dependent on claim 5 reads similarly to claim 22. Claim 26 dependent on claim 5 reads: "an IEEE 802.1x engine for converting the access request to a RADIUS message, for responding to a RADIUS access reject message and for detecting a state failure." Claim 27 dependent on claim 7 reads similarly to

claim 25. All of claims 22, 23 and 25-27 are supported by Zhang et al. paragraphs [0020] – [0021]. Claims 22-23 and 25-27 are not suggested or described by Luo.

For example, the only reference to "failure state" in Luo is [0023] to "repeated authentication failures" which is different from "wireless local area network failure state information via a web request redirect" (claim 22), "detecting a state failure responsive to receipt of an EAP response identity packet and to receipt of a RADIUS access reject message" (claim 25) and so on.

Luo discusses a RADIUS server 110 in the BACKGROUND: "requires that every user have an account at a centralized authentication server, such as a Remote Authentication Dial In User Service (RADIUS) server;" (See Luo paragraph [0013]). Luo discusses a RADIUS server supporting ZCMN at paragraph [0020] and as being responsible for network-to-user authentication and for generating session-specific keys to encrypt air traffic at paragraph [0027]. "It does not [to] enforce user-to-network authentication" which is "handled by the Web authentication server;" (Applicants note an apparent typographical error). Consequently, it is respectfully submitted that Luo teaches away from the subject matter of claims 25-27.

Consequently, applicants respectfully request that the anticipation rejection of claims 22-23 and 25-27 be withdrawn.

Claims 24 and 31

Independent access point claim 24, for example, reads: "means for forwarding an extended authentication protocol failure message packet to the client terminal responsive to a state failure;" (alternative means for receiving responsive to said state failure); "and means for forwarding a web request redirect from said packet filter module to a designated web server for establishing authorized communications following receipt of selected provider information at the designated web server and successful client terminal reconfiguration responsive to authentication." Claim 24, while supported, for

example, by Zhang et al. FIG. 2, is not described by Luo. As discussed above, the only reference to a failure of any kind in Luo is repeated authentication failures at [0023]. Consequently, applicants respectfully request that the anticipation rejection of claim 24 be withdrawn.

Claim 31 dependent on claim 24 relates to ActiveX control/plug-in not suggested or described by Luo's Java applet which, as described above, performs differently.

Claims 28-29

Claims 28-29 dependent on claims 1 and 5 respectively are directed, for example, at defining "information to establish client terminal access to the wireless network" of claims 1 and 5 as "provider selection information responsive to receipt of a provider list web page at the client terminal from said local web server." A provider list web page is not discussed in Luo; the user "launches his web browser" . . . "specifies a non-blank home page" . . . "such as 'http://www.att.com'". Since, for example, a "provider list web page" is not disclosed by Luo, applicants respectfully request the anticipation rejection of claims 28 and 29 be withdrawn.

Conclusion:

Appellants respectfully request that members of the Board reverse the decision of the Examiner rejecting claims 1-31 as anticipated by Luo and allow claims 1-31.

The Commissioner is authorized in this, concurrent, and future replies, to charge payment or credit any overpayment to Deposit Account No. 07-0832 for any additional fees required under 37 C.F.R. § 1.16 or under 37 C.F.R. § 1.17.

Respectfully submitted,

Junbiao Zhang, et al.

By: /Catherine A. Ferguson/

Catherine A. Ferguson, Reg. No. 40,877

Patent Operations
Thomson Licensing LLC
Princeton, New Jersey 08543-5312
(609)734-6440

Date: September 29, 2009

VIII. CLAIMS APPENDIX

1. (Previously presented) A method for enabling a client terminal to access a wireless network, comprising:

receiving an access request from the client terminal;

redirecting the access request to a local web server via a packet traffic filter for filtering packet traffic;

requesting from the client terminal, information to establish client terminal access to the wireless network;

activating, in response to the client terminal access information received from the client terminal, a module that reconfigures the client terminal for authentication using appropriate parameters associated with a configuration arrangement selected by a user; and

authenticating the reconfigured client terminal and allowing access to the wireless network in response to the authentication.

Claim 2 (Previously presented). The method according to claim 1, wherein the wireless network is an IEEE 802.11 compliant wireless local area network (WLAN), and the client terminal is an IEEE 802.1x compliant client terminal.

Claim 3 (Previously presented). The method according to claim 2, wherein the activating step comprises activating an ActiveX control/plug-in installed on the client terminal.

Claim 4 (Original).The method according to claim 2, wherein the activating step comprises downloading to, and activating in, the client terminal an ActiveX control/plug-in.

Claim 5 (Previously presented). An access point for providing a secure

communications session between a client terminal and a wireless network, comprising:

means for receiving an access request from the client terminal;

means for redirecting the access request to a local web server for allowing a reconfigured access to the wireless network via a packet filter means for filtering packet traffic,

means for requesting from the client terminal, information to establish client terminal access to the wireless network;

means for activating, in response to the client terminal access information received from the client terminal, a software module that reconfigures the client terminal for authentication using appropriate parameters associated with a configuration arrangement selected by a user; and

means for authenticating the reconfigured client terminal and allowing access to the wireless network in response to the authentication.

Claim 6 (Original).The access point according to claim 5, wherein the access point complies with the IEEE 802.11 standards and the client terminal is an IEEE 802.1x compliant client terminal.

Claim 7 (Previously presented). A method for configuring a client terminal to provide secure access in a wireless network, comprising:

filtering traffic associated with a request from the client terminal for access to the wireless network, at a packet traffic filter for filtering packet traffic;

redirecting the access request to a designated web server, via said packet traffic filter for filtering packet traffic; and

issuing a provider list web page and a request from the designated web server to the client terminal for provider selection information to establish an

authorized communication.

Claim 8 (Previously presented). The method according to claim 7, wherein the wireless network is an IEEE 802.11 compliant wireless local area network and the client terminal is an IEEE 802.1x compliant client terminal.

Claim 9 (Previously presented). The method according to claim 7, further comprising the designated web server receiving from the client terminal said provider selection information for establishing said authorized communication.

Claim 10 (Previously presented). The method according to claim 9, further comprising the client terminal receiving information corresponding to parameters from the designated web server and including transmission rate information for establishing said authorized communication.

Claim 11 (Previously presented). The method according to claim 9, further comprising the client terminal receiving information corresponding to parameters from the designated web server including user account creation information for establishing said authorized communication.

Claim 12 (Previously presented). The method according to claim 9, further comprising the client terminal receiving information corresponding to parameters from the designated web server including authentication method selection information for establishing said authorized communication.

Claim 13 (Previously presented). The method according to claim 9, further comprising the client terminal receiving information corresponding to parameters from the designated web server including new account creation procedures for establishing said authorized communication.

Claim 14 (Previously presented). The method according to claim 9, further comprising the client terminal receiving information corresponding to parameters from the designated web server including access user terms and conditions of acceptance information for establishing said authorized communication.

Claim 15 (Previously presented). The method according to claim 10, further comprising the client terminal communicating to the designated web server access rate information for establishing said authorized communication.

Claim 16 (Previously presented). The method according to claim 11, further comprising the client terminal communicating web server user account creation information to the designation web server for establishing said authorized communication.

Claim 17 (Previously presented). The method according to claim 12, further comprising the client terminal communicating user access authentication method selection information to the designated web server for establishing said authorized communication.

Claim 18 (Previously presented). The method according to claim 14, further comprising the client terminal communicating user access terms and conditions of acceptance information for establishing said authorized communication.

Claim 19 (Previously presented). The method according to claim 9, whereby authentication is browser based and related to said provider list web page and the method further comprising invoking an ActiveX control to reconfigure the

client terminal.

Claim 20 (Previously presented). The method according to claim 8, whereby authentication is browser based and the method further comprising sending an ActiveX control to configure the client terminal, a software module of said client terminal reconfiguring the client terminal and establishing said authorized communication.

Claim 21 (Previously presented). A mobile terminal, comprising:

means for receiving an extended authentication protocol request identification message packet;

means for forwarding an extended authentication protocol response identity message packet;

means for receiving an extended authentication protocol failure message packet;

means for forwarding a web access request via a packet traffic filter for filtering packet traffic as a web request redirect message;

means for receiving a provider list web page;

means for selecting a provider and means for forwarding selected provider information to a designated web server;

means for receiving an ActiveX control/plug-in from the designated web server to reconfigure said mobile terminal; and

means for reconfiguring said mobile terminal and establishing authorized communications.

Claim 22 (Previously presented). The method as recited in claim 1, the method further comprising

creating a plurality of operational states including a progress state and a failure state, said packet traffic filter receiving wireless local area network

failure state information via a redirect client message and moves a reconfiguration process to said local web server via a web request redirect message.

Claim 23 (Previously presented). The access point as recited in claim 5, the access point creating a plurality of operational states including a progress state and a failure states wherein said packet traffic filter means receives wireless local area network failure state information via a redirect client message and moves a reconfiguration process to said local web server via a web redirect message.

Claim 24 (Previously presented). An access point associated with a communications network, comprising:

means for forwarding an extended authentication protocol request identification message packet to a client terminal;

means for receiving an extended authentication protocol response identity message packet from the client terminal;

means for forwarding an extended authentication protocol failure message packet to the client terminal responsive to a state failure;

means for receiving a re-direct client request from said forwarding means at a packet filter module responsive to said state failure;

alternative means for receiving a request for access to a communications network at said packet filter module responsive to said state failure; and

means for forwarding a web request redirect from said packet filter module to a designated web server for establishing authorized communications following receipt of selected provider information at the designated web server and successful client terminal reconfiguration responsive to authentication.

Claim 25 (Previously presented). The method according to claim 1, further comprising:

detecting a state failure responsive to receipt of an EAP response identity packet and to receipt of a RADIUS access request reject message; and

redirecting the access request to a local web server via said packet traffic filter responsive to one of the packet traffic filter receiving a redirect client request and of receiving a web access request from said client terminal after detection of said state failure.

Claim 26 (Previously presented). The access point according to claim 5, further comprising:

an IEEE 802.1x engine for converting the access request to a RADIUS message, for responding to a RADIUS access reject message and for detecting a state failure; and

said packet traffic filter means redirecting the access request to a local web server responsive to one of the packet traffic filter means receiving a redirect client request from said_IEEE 802.1x engine and of receiving a web access request from said client terminal after the IEEE 802.1x engine detecting said state failure.

Claim 27 (Previously presented). The method according to claim 7, further comprising:

detecting a state failure responsive to receipt of an EAP response identity packet and to receipt of a RADIUS access request reject message; and

redirecting the access request to said designated web server via said packet traffic filter responsive to one of the packet traffic filter receiving a redirect client request and of receiving a web access request from said client terminal after detection of said state failure.

Claim 28 (Previously presented). The method according to claim 1 wherein said information to establish client terminal access to the wireless network comprises provider selection information responsive to receipt of a provider list web page at the client terminal from said local web server.

Claim 29 (Previously presented). The access point according to claim 5 wherein said information to establish client terminal access to the wireless network comprises provider selection information responsive to receipt of a provider list web page at the client terminal from said local web server.

Claim 30 (Previously presented). The mobile terminal according to claim 21 wherein said provider list web page and said ActiveX control/plug-in are received from a local web server in response to receipt of a web request redirect message from an access point.

Claim 31 (Previously presented). The access point according to claim 24 wherein said designated web server transmits an ActiveX control/plug-in for configuring the client terminal responsive to the receipt of selected provider information at the designated web server.

IX. EVIDENCE APPENDIX

None.

X. RELATED PROCEEDINGS APPENDIX

None.